DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/5/2009 has been entered.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Robert Madden (Reg. No. 57,521) on 4 April 2009.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 3.

Replace claims 1, 2, 4 – 7 and 9 – 11 as follows.

1. (Currently Amended):   A method of providing conditional access to an encrypted data

stream ~~with a stream receiving device (12)~~, the method comprising:

        - <u>receiving</u> ~~including~~ encrypted content data <u>at a stream receiving device</u>, the decryption

of which requires temporally changing control words (CW), in [[the]]<u>a</u> data stream;

        - <u>receiving</u> ~~including~~ first decryption control messages (ECM's) in the data stream, each

first decryption control message (ECM) containing at least one of the control words that is

required for decrypting <u>the encrypted</u> content data ~~that is substantially contemporaneous with~~

~~the first decryption control message (ECM) in the stream~~;

        - <u>receiving</u> ~~including~~ second decryption control messages (EMM's) which contain

management information for entitling selected stream receiving devices to decrypt <u>the</u>

<u>encrypted</u> content data from the data stream using control words from the first decryption

control messages (ECM's);

        - <u>receiving</u> ~~including~~ further management information <u>included</u> in at least part of the first

decryption <u>control</u> messages (ECM's) <u>at random based upon a random generator, contained in</u>

<u>at least one of source providers, for supplying said management information</u>;

        - extracting a control word from [[a]] <u>at least one of the</u> first decryption <u>control</u> message

(ECM) from the stream ~~in a stream receiving device (12)~~;

        - together with said extracting, testing whether the <u>at least one</u> first decryption <u>control</u>

message (ECM) contains further management information targeted at the stream receiving

device ~~(12)~~; and

        - indefinitely disabling subsequent decryption of at least part of the stream in the stream

receiving device ~~(12)~~ upon ~~said~~ detection <u>of said testing,</u>

        <u>wherein said further management information specifies a condition upon entitlement</u>

<u>data, said testing comprising searching for entitlement data stored in said stream receiving</u>

device to detect whether any of the searched entitlement data meets said condition, and

performing said disabling if such entitlement data with specified said condition of disabling is

found.

2. (Currently Amended):   A method according to Claim 1, wherein the stream receiving

device (12) contains identification information that individually identifies the stream receiving

device (12), [[said]] first decryption control message (ECM) containing further identification

information, said testing comprising comparing the identification information and the further

identification information.

4. (Currently Amended): A method of generating an encrypted data stream, the method

comprising:

        - including generating encrypted content data at a stream generating device, the

decryption of which requires temporally changing control words, in the data stream;

        - including generating first decryption control messages (ECM's), which contain the

control words, in the data stream;

        - including generating second decryption control messages (EMM's) which contain

management information for entitling selected stream receiving devices to decrypt content data

from the data stream using control words from the first decryption control messages (ECM);

[[and]]

        - including generating further management information in at least part of the first

decryption control messages (ECM's) at random based upon a random generator, contained in

at least one of source providers, for supplying said management information, the further

management information being arranged to target selected stream receiving devices (12) to

indefinitely disable subsequent decryption of at least part of the stream in the stream receiving

device ~~(12)~~; and

      <u>- including said encrypted content data, said first decryption control messages (ECM's),</u>

<u>said first decryption control messages (EMM's) and said further management information in the</u>

<u>data stream,</u>

      <u>wherein said further management information specifies a condition upon entitlement data,</u>

<u>and searching for entitlement data stored in said selected stream receiving devices to detect</u>

<u>whether any of the searched entitlement data meets said condition, and performing the</u>

<u>disabling if such entitlement data with specified said condition of disabling is found</u>.

5. (Currently Amended):   A method according to Claim 4, wherein the further management

information targets the selected stream receiving devices ~~(12)~~ with identification information

corresponding to individual identification information of selected stream receiving devices.

6. (Currently Amended):   A method according to Claim 4, wherein the further management

information targets the selected stream receiving devices ~~(12)~~ with information that specifies a

condition upon a content of entitlement data in said stream receiving devices.

7. (Currently Amended):   A stream receiving device ~~(12)~~ for providing conditional access to

an encrypted data stream, wherein the data stream comprises encrypted content data, the

decryption of which requires temporally changing control words, the data stream further

comprising first decryption control messages (ECM's), which each contain a control word,

~~substantially contemporaneously with the content data that can be decrypted with that control~~

~~word~~, and second decryption control messages (EMM's) which contain management information

for entitling the stream receiving device to decrypt content data from the data stream using
control words from the first decryption control messages (ECM's), the stream receiving device
comprising:

    ~~a circuit (124) arranged~~

    <u>a processor and a circuit configured to perform the functions of:</u>

    - ~~extract~~ <u>extracting</u> a control word from a first decryption message from the stream, and,

    - together with said extracting, to test whether the first ~~encryption~~ <u>decryption control</u>
messages (ECM's) contain further management information targeted at the stream receiving
device ~~(12)~~, the stream receiving device ~~(12)~~ indefinitely disabling subsequent decryption of at
least part of the stream upon ~~said~~ detection <u>of said testing,</u>

        <u>wherein said further management information is included in at least part of the first</u>
<u>decryption control messages (ECM's) at random based upon a random generator, contained in</u>
<u>at least one of source providers, for supplying said management information and specifies a</u>
<u>condition upon entitlement data, said testing comprising searching for entitlement data stored in</u>
<u>said stream receiving device to detect whether any of the searched entitlement data meets said</u>
<u>condition, and performing said disabling if such entitlement data with specified said condition of</u>
<u>disabling is found.</u>

9. (Currently Amended): A stream receiving device according to Claim 7, wherein said testing
whether the further management information is targeted at the stream receiving device
comprises searching for entitlement data stored in said stream receiving device ~~(12)~~ that meets
a condition specified in the further management information.

10. (Currently Amended): A smart card for use in a stream receiving device according to Claim 7, the smart card comprising a processor (124) and an entitlement memory (126), the processor (124) being programmed to:

- extract a control word from a first decryption control message (ECM) from the stream and to supply the control word for use in decrypting content data;

- update the entitlement memory using information from a second decryption control message (EMM);

- together with said extracting, test whether the first ~~encryption~~ decryption control message (ECM) ~~messages (ECM's)~~ contains further management information targeted at the stream receiving device, wherein the further management information is included in the first decryption control messages (ECM's) at random based upon a random generator, contained in at least one of source providers, for supplying said management information, and

- indefinitely disable subsequent supply of control words of at least part of the stream upon said detection.

11. (Currently Amended): A stream generating device for generating an encrypted data stream, the stream generating device comprising:

     a processor and a circuit configured to:

     - generate a source of content data, comprising an encryption unit for encrypting the content data so that temporally changing control words are required;

          - generate a source of first decryption control messages, that generates first control word messages in the stream containing control words for decrypting the content data; and

          - generate a source of access management information, that generates first control word messages in the stream containing management information for entitling selected stream

receiving devices to decrypt content data, the source of access management information being coupled to the source of first decryption control messages, the source of first decryption control messages being arranged to include further management information in at least part of the first decryption <u>control</u> messages <u>at random based upon a random generator, contained in at least one of source providers, for supplying said management information</u>, the further management information being arranged to target selected stream receiving devices to indefinitely disable subsequent decryption of at least part of the stream in the stream receiving device<u>,</u>

   <u>wherein said further management information specifies a condition upon entitlement data and searching for entitlement data stored in said selected stream receiving devices to detect whether any of the searched entitlement data meets said condition, and performing the disabling if such entitlement data with specified said condition of disabling is found</u>.

Allowable Subject Matter

   Claims 1 – 2 and 4 – 11 are allowed.

   The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations recited in claims 1, 4, 7 and 11 (& associated dependent claims).

   The present invention is directed to a method for providing conditional access to an encrypted data stream and comprises receiving encrypted content data at a stream receiving device, the decryption of which requires temporally changing control words (CW), in a data stream; receiving first decryption control messages (ECM's) in the data stream, each first decryption control message (ECM) containing at least one of the control words that is required for decrypting the encrypted content data; receiving second decryption control messages

(EMM's) which contain management information for entitling selected stream receiving devices to decrypt the encrypted content data from the data stream using control words from the first decryption control messages (ECM's). No singular art disclosing, nor motivation to combine has been found to anticipate or render obvious the claimed invention of receiving further management information included in at least part of the first decryption control messages (ECM's) at random based upon a random generator, contained in at least one of source providers, for supplying said management information; together with said extracting, testing whether the at least one first decryption control message (ECM) contains further management information targeted at the stream receiving device; and indefinitely disabling subsequent decryption of at least part of the stream in the stream receiving device upon detection of said testing, wherein said further management information specifies a condition upon entitlement data, said testing comprising searching for entitlement data stored in said stream receiving device to detect whether any of the searched entitlement data meets said condition, and performing the disabling if such entitlement data with specified said condition of disabling is found.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

　　　　Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

　　　　/Longbit Chai/

Primary Patent Examiner
　　Art Unit 2431
　　4/02/2009